STAT

3. AGENCY INFORMATION SECURITY PROGRAM

SYNOPSIS. This regulation implements Executive Order 12356 within the Agency. It establishes the Agency program for classifying, downgrading, declassifying, marking, and safeguarding national security information.

a. INTRODUCTION

(1) Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, National Security Information, provides the only basis for classifying information.

(2) The National Security Council (NSC) may review all matters concerning the implementation of Executive Order 12356, and the NSC provides overall policy direction for the executive branch information security program.

(3) The Administrator of General Services is responsible for implementing and monitoring the information security program established by the order. This responsibility is delegated to the Information Security Oversight Office (ISOO), which has a full-time director appointed by the Administrator subject to approval by the President.

(4) The Director, ISOO (D/ISOO):

(a) Develops, in consultation with the agencies that handle classified information, and promulgates, subject to NSC approval, directives for the implementation of the order which are binding on the agencies.

(b) Oversees the agencies' actions to ensure compliance with the order and implementing directives.

(c) Considers and takes action on complaints and suggestions from persons within or outside the Government regarding the administration of the information security program.

(5) The D/ISOO has the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

(6) The Attorney General, upon request by the head of an agency or D/ISOO, will render an interpretation of the order with respect to any question arising in the course of its administration.

b. GENERAL

(1) The provisions of this regulation apply to the Central Intelligence Agency, including the Office of the Director of Central Intelligence, hereinafter referred to as the "Agency."

(2) This regulation establishes, effective 1 August 1982, the Agency information security program pursuant to Executive Order 12356 and related ISOO directives.

(3) The program will be executed in full conformity with the order, the National Security Act of 1947, as amended, and the Central Intelligence Agency Act of 1949, as amended (50 U.S.C. 403a et seq.), as well as with other applicable provisions of law, regulations, and directives.

(4) The provisions of any previously published regulatory issuance inconsistent with the provisions of this regulation are superseded.

(5) A copy of this regulation and other regulations adopted to carry out this program will be submitted to the ISOO. The D/ISOO will require any regulation or guideline to be changed if it is not consistent with the order or implementing directives. Any such decision by the D/ISOO may be appealed to the NSC. The regulation or guideline will remain in effect until the appeal is decided.

(6) Unclassified regulations that establish Agency information security policy will be published in the Federal Register to the extent that these regulations affect members of the public.

(7) The D/ISOO has the authority to conduct onsite review of the Agency information security program and to require such reports, information, and other cooperation as necessary to fulfill his or her responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the Director of Central Intelligence (DCI) may deny access. The D/ISOO may appeal such denials to the NSC. The denial will remain in effect until the appeal is decided.

c. SANCTIONS

(1) If the D/ISOO finds that a violation of E.O. 12356 or its implementing directives may have occurred, he or she will make a report to the DCI or the senior Agency official designated in paragraph e(1) below so that corrective steps may be taken, as appropriate.

(2) Officials and employees of the Agency and Agency contractors, licensees, and grantees will be subject to appropriate sanctions if they:

(a) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12356 or predecessor orders.

(b) Knowingly and willfully classify or continue the classification of information in violation of the order or any implementing directive.

(c) Knowingly and willfully violate any other provision of the order or implementing directive.

(3) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and Agency regulations. Sanctions to contractors will be in accordance with applicable law, Agency regulations, and the terms and conditions of the contract.

(4) The DCI or the senior Agency official designated in paragraph e(1) below will ensure that appropriate and prompt corrective action is taken whenever a violation under paragraph c(2) above occurs. Either will ensure that the D/ISOO is notified in accordance with procedures established by the D/ISOO whenever a violation under paragraph c(2)(a) or (b) occurs.

d. POLICY AND PROCEDURES. [redacted] implements the program established by this regulation and should be used in conjunction with this regulation and other regulatory issuances published pursuant to the program.

e. RESPONSIBILITIES

(1) The Deputy Director for Administration (DDA) is the senior Agency official responsible for the direction and administration of the Agency information security program, which will include an active oversight and security education program to ensure effective implementation of Section 5.3(a) of the order. As the senior official for the information security program, the DDA is the sole alternate to the DCI for delegating original Top Secret classification authority.

(2) The Director of Information Services (D/OIS), DDA, is responsible for general management of the information security program. The D/OIS is the Agency focal point for contact with the ISOO. On information security program matters, the D/OIS is the focal point for contact with the NSC and, through the Office of General Counsel, with the Department of Justice.

(3) The Director of Security is responsible for the safeguarding provisions of the program, as specified in [redacted]

(4) The Chief, Records Management Division, Office of Information Services, DDA, is responsible for the classification provisions and general administration of the program, as specified in [redacted]

(5) The Chief, Information and Privacy Division, Office of Information Services, DDA, is responsible for the mandatory review provisions of the program, as specified in [redacted]

~~4. Reserved.~~ Delete per [redacted]

STAT

TRANSMITTAL SLIP | DATE 23 June 83

TO

ROOM NO. 4E70 | BUILDING

REMARKS:

See what you think?

STAT

FROM:

ROOM NO.

FORM NO. 1 FEB 55 241 REPLACES FORM 36-8 WHICH MAY BE USED. (47)